



GA4/2131

#2

Attorney Docket No. Q66100
PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Kazuo KURODA, et al.

Appln. No.: 09/944,179

Group Art Unit: 2131

Confirmation No.: 9852

Examiner: Not Yet Assigned

Filed: September 4, 2001

For: INFORMATION SENDING METHOD AND INFORMATION SENDING
APPARATUS, INFORMATION RECEIVING APPARATUS AND INFORMATION...

SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
Washington, D.C. 20231

RECEIVED
NOV 16 2001
Technology Center 2100

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to
priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to
acknowledge receipt of said priority document.

Respectfully submitted,

Darryl Mexic
Registration No. 23,063

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, D.C. 20037-3213
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

Enclosures: Japan 2000-267612

Date: November 13, 2001



日 本 国 特 許 庁
JAPAN PATENT OFFICE

Kazuo KURODA, et al.
Filed: September 4, 2001
Q66100 Appln. No.: 09/944,179
Group Art Unit: 2131
(202) 293-7060 1 of 1

#2

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年 9月 4日

出 願 番 号
Application Number:

特願2000-267612

出 願 人
Applicant(s):

パイオニア株式会社

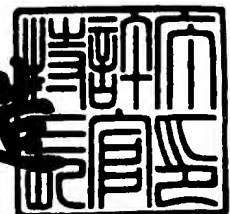
RECEIVED
NOV 16 2001
Technology Center 2100

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月17日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3072627

【書類名】 特許願

【整理番号】 55P0047

【提出日】 平成12年 9月 4日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00 353
G06F 13/00 352
G06F 13/00

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 黒田 和男

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 守山 義明

【発明者】

【住所又は居所】 東京都大田区大森西4丁目15番5号 パイオニア株式会社 大森工場内

【氏名】 橋本 隆

【発明者】

【住所又は居所】 東京都大田区大森西4丁目15番5号 パイオニア株式会社 大森工場内

【氏名】 内藤 明彦

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【代理人】

【識別番号】 100083839

【弁理士】

【氏名又は名称】 石川 泰男

【電話番号】 03-5443-8461

【手数料の表示】

【予納台帳番号】 007191

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9102133

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報送信装置及び情報送信方法、情報受信装置及び情報受信方法、情報伝送システム及び情報伝送方法並びに情報記録媒体

【特許請求の範囲】

【請求項 1】 他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態では、他の情報と非同期の状態では情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して複数の情報処理装置が相互に接続されている情報伝送システムにおいて、

各前記情報処理装置は、

前記情報を暗号化するための暗号処理情報を前記第 2 伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受するための第 2 授受手段と、

各前記情報処理装置間で授受すべき前記情報である特定情報を前記暗号処理情報を用いて暗号化して得られる暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受するための第 1 授受手段と、

を夫々備えることを特徴とする情報伝送システム。

【請求項 2】 他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態では、他の情報と非同期の状態では情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して複数の情報処理装置が相互に接続されている情報伝送システムにおける情報伝送方法において、

前記情報を暗号化するための暗号処理情報を前記第 2 伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受する第 1 授受工程と、

各前記情報処理装置間で授受すべき前記情報である特定情報を前記暗号処理情報を用いて暗号化して得られる暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受する第 2 授受工程と、

を備えることを特徴とする情報伝送方法。

【請求項 3】 他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態では、他の情報と非同期の状態では情報を伝送する第 1 伝送態様であって前記第 2 伝

送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して、情報受信装置に対して前記情報を送信する情報送信装置において、

前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化手段と、

前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 1 送信手段と、

前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化手段と、

前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 2 送信手段と、

を備えることを特徴とする情報送信装置。

【請求項 4】 請求項 3 に記載の情報送信装置において、

前記特定情報は A V (Audio Visual) 情報であると共に、

前記暗号処理情報は当該 A V 情報を暗号化するための暗号化キー及び暗号化テーブルであることを特徴とする情報送信装置。

【請求項 5】 請求項 3 又は 4 に記載の情報送信装置において、

前記伝送手段は、I E E E (Institute of Electrical and Electronic Engineers) 1 3 9 4 規格に準拠して前記暗号化特定情報及び前記暗号化処理情報を伝送すると共に、

前記第 1 伝送態様は前記 I E E E 1 3 9 4 規格におけるアシンクロナス伝送モードであり、前記第 2 伝送態様は当該 I E E E 1 3 9 4 規格におけるアイソクロナス伝送モードであることを特徴とする情報送信装置。

【請求項 6】 他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態では情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して、情報受信装置に対して前記情報を送信する情報送信方法において、

前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化工程と、

前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 1 送信工程と、

前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化工程と、

前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 2 送信工程と、

を備えることを特徴とする情報送信方法。

【請求項 7】 請求項 3 から 5 のいずれか一項に記載の情報送信装置から送信された前記暗号化特定情報を受信する情報受信装置であって、

前記暗号化特定情報を前記伝送手段から取得する第 1 取得手段と、

前記暗号化処理情報を前記伝送手段から取得する第 2 取得手段と、

前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第 2 解読手段と、

前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する第 1 解読手段と、

を備えることを特徴とする情報受信装置。

【請求項 8】 請求項 7 に記載の情報受信装置において、

前記生成された特定情報を予め設定された記録媒体に記録する記録手段を更に備えることを特徴とする情報受信装置。

【請求項 9】 請求項 3 から 5 のいずれか一項に記載の情報送信装置から送信された前記暗号化特定情報を受信する情報受信装置における情報受信方法であって、

前記暗号化特定情報を前記伝送手段から取得する第 1 取得工程と、

前記暗号化処理情報を前記伝送手段から取得する第 2 取得工程と、

前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第 2 解読工程と、

前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する第 1 解読工程と、

を備えることを特徴とする情報受信方法。

【請求項 1 0】 他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段と、当該伝送手段を介して前記情報を送信する情報送信装置と、前記送信された情報を前記伝送手段を介して受信すると情報受信装置と、を含む情報伝送システムにおいて、

前記情報送信装置は、

前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化手段と、

前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 1 送信手段と、

前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化手段と、

前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 2 送信手段と、を備えると共に、

前記情報受信装置は、

前記暗号化特定情報を前記伝送手段から取得する第 1 取得手段と、

前記暗号化処理情報を前記伝送手段から取得する第 2 取得手段と、

前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第 2 解読手段と、

前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する第 2 解読手段と、

を備えることを特徴とする情報伝送システム。

【請求項 1 1】 他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を伝送する第 1 伝送態様であって前記第 2

伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかに
より前記情報を伝送することが可能な伝送手段を介して、情報受信装置に対して
前記情報を送信する情報送信装置に含まれる送信コンピュータを、

前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信
すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化
手段、

前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介
して前記情報受信装置に送信する第 1 送信手段、

前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化手段
、及び、

前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介
して前記情報受信装置に送信する第 2 送信手段、

として機能させることを特徴とする送信制御プログラムが前記送信コンピュ
ータで読取可能に記録された情報記録媒体。

【請求項 1 2】 請求項 1 1 に記載の情報送信装置から送信された前記暗号
化特定情報を受信する情報受信装置に含まれる受信コンピュータを、

前記暗号化特定情報を前記伝送手段から取得する第 1 取得手段、

前記暗号化処理情報を前記伝送手段から取得する第 2 取得手段、

前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第 2 解
読手段、及び、

前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定
情報を生成する第 1 解読手段、

として機能させることを特徴とする受信制御プログラムが前記受信コンピュ
ータで読取可能に記録された情報記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、情報送信装置及び情報送信方法、情報受信装置及び情報受信方法、
情報伝送システム及び情報伝送方法並びに情報記録媒体の技術分野に属し、より

詳細には、暗号化された情報及び当該暗号化に用いられた暗号処理情報を共に送受信することが可能な情報送信装置及び情報送信方法、情報受信装置及び情報受信方法、当該情報送信装置及び情報受信装置を含む情報伝送システム及び情報伝送方法並びに送信制御プログラム又は受信制御プログラムが記録された情報記録媒体の技術分野に属する。

【 0 0 0 2 】

【従来の技術】

従来、放送電波を用いて放送されている音楽情報等を放送受信用のセットトップボックスにより受信し、これを光ディスク等の記録媒体に情報記録装置を用いて記録することが行われている。

【 0 0 0 3 】

一方、近年では、画像圧縮技術及び高密度記録技術の発展に鑑み、一本の映画等を放送電波を介して配信し、これを例えばDVD（従来のCD（Compact Disc）よりも数倍記録容量を高めた光ディスク）等の記録容量の高い情報記録媒体に記録することが実行されている。

【 0 0 0 4 】

ここで、上述したような音楽情報等の配信においては、当該音楽情報等における著作権をどのように保護するかが問題となっており、この点、従来では、当該セットトップボックスから上記情報記録装置に至るまでの伝送経路上及び情報記録媒体への記録時の双方においていわゆる暗号化を行った上で配信又は記録を行うこととされていた。

【 0 0 0 5 】

このとき、近年においては、当該セットトップボックスと情報記録装置との間においていわゆるIEEE 1394規格（正式名称は、「IEEE Std.1394-1995 IEEE Standard for a High Performance Serial Bus」である。）に準拠した伝送態様で音楽情報等が伝送される場合が多いが、この場合には、当該セットトップボックスと情報記録装置との間では、著作権保護のための規格としていわゆるDTC P（Digital Transmission Copy Protection）規格に基づいた著作権保護が為されている場合が多かった。

【 0 0 0 6 】

一方、上記 D T C P 規格においては、予め設定されている暗号化のための暗号処理情報を用いて暗号化した上記音楽情報等をセットトップボックスから情報記録装置に伝送すると共に、当該暗号処理情報自体も暗号化し、それをやはりセットトップボックスから情報記録装置に伝送し、当該情報記録装置においては伝送された暗号処理情報を用いて音楽情報等の暗号化を解読して記録する構成とされている。

【 0 0 0 7 】

そして、従来においては、上記暗号化された音楽情報等は I E E E 1 3 9 4 規格におけるいわゆるアイソクロナス伝送モードを用いて D T C P 規格により伝送されていた。

【 0 0 0 8 】

なお、上記 D T C P 規格については、インターネット上で D T L A (Digital Transmission Licensing Administrator) によりその内容が詳細に公開されている (U R L は、HYPERLINK <http://www.dtcp.com/> <http://www.dtcp.com> である。) 。

【 0 0 0 9 】

【発明が解決しようとする課題】

しかしながら、上記従来構成においては、暗号化された音楽情報等が I E E E 1 3 9 4 規格におけるアイソクロナス伝送モードを用いて D T C P 規格により伝送されているが、一方、現在 D T L A においては当該 D T C P 規格による情報伝送における伝送速度は記録後の音楽情報等の再生速度と同一の速度しか使用認可されておらず、結局 I E E E 1 3 9 4 規格の特性を最大限に活用して暗号化された音楽情報等を高速にセットトップボックスから情報記録装置に伝送することができないという問題点があった。

【 0 0 1 0 】

また、上記従来構成においては、D T C P 規格により伝送中は著作権の保護が図られていると言えるが、セットトップボックスにおける D T C P 規格に基づいた暗号化前及び情報記録装置における解読後においては、音楽情報等が暗号化

されていない状態となり得るため、夫々の段階では著作権情報の保護が不十分であるという問題点があった。

【0011】

そこで、本発明は、上記の各問題点に鑑みて為されたもので、その課題は、暗号処理情報を用いて暗号化された音楽情報等を伝送する場合に、当該音楽情報等を暗号化された状態で秘匿性を高めつつ高速且つ大量に伝送することが可能な情報送信装置及び情報送信方法、情報受信装置及び情報受信方法、当該情報送信装置及び情報受信装置を含む情報伝送システム及び情報伝送方法並びに送信制御プログラム又は受信制御プログラムが記録された情報記録媒体を提供することにある。

【0012】

【課題を解決するための手段】

上記の課題を解決するために、請求項1に記載の発明は、他の情報と同期した状態で情報を伝送する第2伝送態様、又は、他の情報と非同期の状態では情報を伝送する第1伝送態様であって前記第2伝送態様による伝送よりも高速で前記情報を伝送する第1伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して複数の情報処理装置が相互に接続されている情報伝送システムにおいて、各前記情報処理装置は、前記情報を暗号化するための暗号処理情報を前記第2伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受するためのインタフェース部等の第2授受手段と、各前記情報処理装置間で授受すべき前記情報である特定情報を前記暗号処理情報を用いて暗号化して得られる暗号化特定情報を、前記第1伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受するためのインタフェース部等の第1授受手段と、を夫々備える。

【0013】

よって、暗号化特定情報を高速の第1伝送態様で送受信すると共に、暗号処理情報を第2伝送態様で送受信するので、情報処理装置間で送受信すべき特定情報を暗号化された状態で高速且つ大量に送受信することができる。

【0014】

また、送信前に特定情報が暗号化されるので、当該特定情報の秘匿性を高めつつ送信することができる。

【 0 0 1 5 】

上記の課題を解決するために、請求項 2 に記載の発明は、他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して複数の情報処理装置が相互に接続されている情報伝送システムにおける情報伝送方法において、前記情報を暗号化するための暗号処理情報を前記第 2 伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受する第 1 授受工程と、各前記情報処理装置間で授受すべき前記情報である特定情報を前記暗号処理情報を用いて暗号化して得られる暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して当該情報処理装置間で相互に授受する第 2 授受工程と、を備える。

【 0 0 1 6 】

よって、暗号化特定情報を高速の第 1 伝送態様で送受信すると共に、暗号処理情報を第 2 伝送態様で送受信するので、情報処理装置間で送受信すべき特定情報を暗号化された状態で高速且つ大量に送受信することができる。

【 0 0 1 7 】

また、送信前に特定情報が暗号化されるので、当該特定情報の秘匿性を高めつつ送信することができる。

【 0 0 1 8 】

上記の課題を解決するために、請求項 3 に記載の発明は、他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能なシリアルバス等の伝送手段を介して、情報受信装置に対して前記情報を送信する情報送信装置において、前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生

成する暗号化部等の第1暗号化手段と、前記生成された暗号化特定情報を、前記第1伝送態様により前記伝送手段を介して前記情報受信装置に送信するインタフェース部等の第1送信手段と、前記暗号処理情報自体を暗号化し、暗号化処理情報を生成するDTC P暗号化部等の第2暗号化手段と、前記生成された暗号化処理情報を、前記第2伝送態様により前記伝送手段を介して前記情報受信装置に送信するインタフェース部等の第2送信手段と、を備える。

【0019】

よって、暗号化特定情報を高速の第1伝送態様で送信すると共に、暗号化処理情報を第2伝送態様で送信するので、情報受信装置に送信すべき特定情報を暗号化された状態で高速且つ大量に送信することができる。

【0020】

また、送信前に特定情報が暗号化されるので、当該特定情報の秘匿性を高めつつ情報受信装置に送信することができる。

【0021】

上記の課題を解決するために、請求項4に記載の発明は、請求項3に記載の情報送信装置において、前記特定情報はA V情報であると共に、前記暗号処理情報は当該A V情報を暗号化するための暗号化キー及び暗号化テーブルであるように構成される。

【0022】

よって、必要なA V情報を秘匿性を高めつつ高速且つ大量に送信することができる。

【0023】

上記の課題を解決するために、請求項5に記載の発明は、請求項3又は4に記載の情報送信装置において、前記伝送手段は、IEEE 1394規格に準拠して前記暗号化特定情報及び前記暗号化処理情報を伝送すると共に、前記第1伝送態様は前記IEEE 1394規格におけるアシンクロナス伝送モードであり、前記第2伝送態様は当該IEEE 1394規格におけるアイソクロナス伝送モードであるように構成される。

【0024】

よって、アシンクロナス伝送モードで暗号化特定情報を送信するので、当該特定情報を I E E E 1 3 9 4 規格における最大伝送速度で情報受信装置に送信することができる。

【 0 0 2 5 】

上記の課題を解決するために、請求項 6 に記載の発明は、他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能なシリアルバス等の伝送手段を介して、情報受信装置に対して前記情報を送信する情報送信方法において、前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化工程と、前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 1 送信工程と、前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化工程と、前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 2 送信工程と、を備える。

【 0 0 2 6 】

よって、暗号化特定情報を高速の第 1 伝送態様で送信すると共に、暗号化処理情報を第 2 伝送態様で送信するので、情報受信装置に送信すべき特定情報を暗号化された状態で高速且つ大量に送信することができる。

【 0 0 2 7 】

また、送信前に特定情報が暗号化されるので、当該特定情報の秘匿性を高めつつ情報受信装置に送信することができる。

【 0 0 2 8 】

上記の課題を解決するために、請求項 7 に記載の発明は、請求項 3 から 5 のいずれか一項に記載の情報送信装置から送信された前記暗号化特定情報を受信する情報受信装置であって、前記暗号化特定情報を前記伝送手段から取得するインタフェース部等の第 1 取得手段と、前記暗号化処理情報を前記伝送手段から取得するインタフェース部等の第 2 取得手段と、前記取得された暗号化処理情報を解読

し、前記暗号処理情報を生成するDTCF復号部等の第2解読手段と、前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する解読部等の第1解読手段と、を備える。

【0029】

よって、伝送手段から取得された暗号化処理情報を解読して得られた暗号処理情報を用いて暗号化特定情報を解読するので、高速且つ大量に特定情報を受信することができると共に、特定情報の秘匿性を高めつつこれを受信することができる。

【0030】

上記の課題を解決するために、請求項8に記載の発明は、請求項7に記載の情報受信装置において、前記生成された特定情報を予め設定された記録媒体に記録する記録手段を更に備える。

【0031】

よって、秘匿性の高い特定情報を高速に取得して記録媒体に記録することができる。

【0032】

上記の課題を解決するために、請求項9に記載の発明は、請求項3から5のいずれか一項に記載の情報送信装置から送信された前記暗号化特定情報を受信する情報受信装置における情報受信方法であって、前記暗号化特定情報を前記伝送手段から取得する第1取得工程と、前記暗号化処理情報を前記伝送手段から取得する第2取得工程と、前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第2解読工程と、前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する第1解読工程と、を備える。

【0033】

よって、伝送手段から取得された暗号化処理情報を解読して得られた暗号処理情報を用いて暗号化特定情報を解読するので、高速且つ大量に特定情報を受信することができると共に、特定情報の秘匿性を高めつつこれを受信することができる。

【0034】

上記の課題を解決するために、請求項 1 0 に記載の発明は、他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段と、当該伝送手段を介して前記情報を送信する情報送信装置と、前記送信された情報を前記伝送手段を介して受信すると情報受信装置と、を含む情報伝送システムにおいて、前記情報送信装置は、前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化手段と、前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 1 送信手段と、前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化手段と、前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 2 送信手段と、を備えと共に、前記情報受信装置は、前記暗号化特定情報を前記伝送手段から取得する第 1 取得手段と、前記暗号化処理情報を前記伝送手段から取得する第 2 取得手段と、前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第 2 解読手段と、前記生成された暗号化処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する第 2 解読手段と、を備える。

【 0 0 3 5 】

よって、暗号化特定情報を高速の第 1 伝送態様で送受信すると共に、暗号化処理情報を第 2 伝送態様で送受信するので、情報受信装置に伝送すべき特定情報を暗号化された状態で高速且つ大量に送受信することができる。

【 0 0 3 6 】

また、送信前に特定情報が暗号化されると共に受信後にこれを解読して暗号化特定情報の解読に用いるので、当該特定情報の秘匿性を高めつつその送受信を実行することができる。

【 0 0 3 7 】

上記の課題を解決するために、請求項 1 1 に記載の発明は、他の情報と同期した状態で情報を伝送する第 2 伝送態様、又は、他の情報と非同期の状態で情報を

伝送する第 1 伝送態様であって前記第 2 伝送態様による伝送よりも高速で前記情報を伝送する第 1 伝送態様のいずれかにより前記情報を伝送することが可能な伝送手段を介して、情報受信装置に対して前記情報を送信する情報送信装置に含まれる送信コンピュータを、前記情報を暗号化するための暗号処理情報を用いて、当該情報受信装置に送信すべき前記情報である特定情報を暗号化し暗号化特定情報を生成する第 1 暗号化手段、前記生成された暗号化特定情報を、前記第 1 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 1 送信手段、前記暗号処理情報自体を暗号化し、暗号化処理情報を生成する第 2 暗号化手段、及び、前記生成された暗号化処理情報を、前記第 2 伝送態様により前記伝送手段を介して前記情報受信装置に送信する第 2 送信手段、として機能させるための送信制御プログラムが前記送信コンピュータで読取可能に記録されている。

【 0 0 3 8 】

よって、暗号化特定情報を高速の第 1 伝送態様で送信すると共に、暗号化処理情報を第 2 伝送態様で送信するように送信コンピュータを機能させるので、情報受信装置に送信すべき特定情報を暗号化された状態で高速且つ大量に送信することができる。

【 0 0 3 9 】

また、送信前に特定情報が暗号化されるように当該送信コンピュータを機能させるので、当該特定情報の秘匿性を高めつつ情報受信装置に送信することができる。

【 0 0 4 0 】

上記の課題を解決するために、請求項 1 2 に記載の発明は、請求項 1 1 に記載の情報送信装置から送信された前記暗号化特定情報を受信する情報受信装置に含まれる受信コンピュータを、前記暗号化特定情報を前記伝送手段から取得する第 1 取得手段、前記暗号化処理情報を前記伝送手段から取得する第 2 取得手段、前記取得された暗号化処理情報を解読し、前記暗号処理情報を生成する第 2 解読手段、及び、前記生成された暗号処理情報を用いて前記暗号化特定情報を解読し、前記特定情報を生成する第 1 解読手段、として機能させるための受信制御プログラムが前記受信コンピュータで読取可能に記録されている。

【 0 0 4 1 】

よって、伝送手段から取得された暗号化処理情報を解読して得られた暗号処理情報を用いて暗号化特定情報を解読するように受信コンピュータを機能させるので、高速且つ大量に特定情報を受信することができると共に、特定情報の秘匿性を高めつつこれを受信することができる。

【 0 0 4 2 】

【発明の実施の形態】

次に、本発明に好適な実施の形態について、図面に基づいて説明する。

【 0 0 4 3 】

なお、以下に説明する実施の形態は、放送電波を介して配信される音楽情報等の記録情報をセットトップボックスにより受信し、これを I E E E 1 3 9 4 規格に準拠したシリアルバスを介してレコーダに伝送し、更に当該レコーダにおいて記録可能な光ディスクである D V D - R (DVD - Recordable) に対して記録する情報伝送システムに対して本発明を適用した場合の実施の形態である。

【 0 0 4 4 】

(I) I E E E 1 3 9 4 規格について

先ず、具体的な実施形態について説明する前に、実施形態に係る記録情報が伝送される際に準拠する上記 I E E E 1 3 9 4 規格の概要について説明する。

【 0 0 4 5 】

一般に、当該 I E E E 1 3 9 4 規格においては、複数の情報処理装置（以下、単にノードと称する。）間をシリアルバスにより接続し、これら各ノード間で複数チャンネル分（当該規格においては、一のシリアルバスで接続されている系内では最大で 6 3 個の異なるチャンネルを用いて情報伝送できることが規格化されている。）の情報伝送を時分割的に実行するように規格化されている。

【 0 0 4 6 】

ここで、I E E E 1 3 9 4 規格（以下、単にシリアルバス規格と称する。）では、既にシリアルバスで相互に接続されているノード群に新たに他のノードを接続する場合（すなわち、バス接続時）又は上記ノード群から一のノードの接続を取り外す場合（すなわち、バス開放時）において、いわゆるバスリセットと称さ

れるシリアルバスの初期化が実行されることが規格化されている。そして、当該バスリセットに伴って以下の処理が実行され、新たなシリアルバスの接続形態（以下、当該接続形態をトポロジと称する。）が構築される。

（１）バスリセットの発生に伴い、当該バスリセットの発生を検出したノード（すなわち、新たに他のノードが接続されたノード又はそれまでの接続が切り離されたノード）がシリアルバスに接続されている全てのノードに対してバスリセットが発生したことを示すバスリセット信号を送出する。

（２）次に、バスリセット後、各ノードをツリー上に接続するためのツリー識別を行う。そして、当該接続されたツリーの頂点に位置するノードをルートノードとして認識する。

（３）次に、認識されたルートノードが、各ノードをツリー系内で識別するための各ノード毎に固有の識別番号（ＩＤ番号）を当該各ノードに認識させる。

（４）次に、当該形成されたツリー内にある全てのノードの通信状態（具体的には、各ノードの使用チャンネル及び後述する伝送占有時間）を管理し、他のノードが識別可能に現在の使用チャンネル及び現在各ノードにおいて占有されている伝送占有時間を表示するノードであるＩＲＭ（Isochronous Resource Manager）ノードを設定する。

（５）最後に、全てのノードの情報伝送状態を統括するノードであるバスマネージャノードを設定する。

【 0 0 4 7 】

以上の五段階の処理を経て、バスリセット後の新たなトポロジが構成される。

【 0 0 4 8 】

そして、トポロジの構成後に実際に情報を伝送する場合には、当該情報の伝送を開始しようとするノードである伝送ノードは、上記ＩＲＭノードに対して現在の他のノードによる通信状態を照会し、自己が使用したいチャンネル及び伝送占有時間が使用可能であるならば、当該伝送ノードは情報を伝送する権利を獲得し（より具体的には、伝送ノードが使用するチャンネル及び後述する伝送占有時間を当該伝送ノードが確保して）情報伝送を開始する。このとき、当該情報伝送の直前に、当該伝送ノードは、上記ＩＲＭノードにおける通信状態の表示を書き換

える旨（すなわち、当該伝送ノードが情報伝送を開始することによりシリアルバス上の使用中チャンネル及び伝送占有時間が変化するので、この変化後の新しい通信状態に当該表示内容を書き換える必要がある。）をIRMノードに伝送し、これを受けたIRMノードはその表示内容を更新する処理を夫々実行する。この後は、当該更新後の表示内容が他のノードから夫々参照することが可能となるのである。

【 0 0 4 9 】

次に、上記伝送占有時間について略説する。

【 0 0 5 0 】

IEEE 1394規格においては、各ノードからの情報はアイソクロナスサイクル（ここで、「サイクル」とは、シリアルバス上を時分割的に分割して形成される一のサイクルをいう。）と称される単位毎に纏められて送信される。このアイソクロナスサイクルには、他のアイソクロナスサイクル内に含まれる情報と同期して伝送される情報（具体的には、画像情報又はオーディオ情報等）が含まれるアイソクロナス伝送領域と、他の情報とは無関係に非同期で伝送される情報（具体的には、上記画像情報又はオーディオ情報の出力等を制御するための制御情報等）が含まれるアシンクロナス伝送領域とが含まれている。そして、このアイソクロナス伝送領域内の情報が異なったチャンネル毎に時分割されており、夫々のチャンネル毎に異なった情報が伝送される。ここで、アイソクロナス伝送領域を用いて情報を伝送する場合をアイソクロナス伝送モードと称し、一方、アシンクロナス伝送領域を用いて情報を伝送する場合をアシンクロナス伝送モードと称する。

【 0 0 5 1 】

このとき、当該アイソクロナス伝送領域においては、一のアイソクロナスサイクル内におけるアイソクロナス伝送領域の時間的長さが最大で100 μ secであることが規格化されており、従って、一のアイソクロナス伝送領域内の各チャンネルに割り当てられる情報がその伝送のために占有する時間の合計も100 μ sec以下とする必要がある。この時、当該一のチャンネルがアイソクロナスサイクル内で占有する伝送時間が上記伝送占有時間である。

【 0 0 5 2 】

なお、この伝送占有時間は、場合によってはシリアルバスの使用帯域と称されることもあり、また、シリアルバスの使用容量と称される場合もある。一方、一のアイソクロナスサイクル内において、アイソクロナス伝送領域の長さが100 μ sec未満（零の場合も含む。）であるときは、当該アイソクロナス伝送領域以外のアイソクロナスサイクル内の時間は専らアシンクロナス伝送領域として用いられる。

【 0 0 5 3 】

次に、上記シリアルバス規格についてより具体的に図1乃至図3を用いて説明する。

【 0 0 5 4 】

なお、図1は当該シリアルバス規格におけるトポロジの一形態を例示する図であり、図2はシリアルバス上の伝送形態を例示する図であり、図3はアイソクロナスサイクルの構成を示す図である。

【 0 0 5 5 】

上記シリアルバス規格は、現存する又は将来考えられる種々の電気製品を含む情報処理装置全てをシリアルに接続し、相互に情報の授受を行おうとするためのシリアルバスの規格である。

【 0 0 5 6 】

より具体的には、各ノードの接続時の設定が全て自動で行なわれ、更に電源を断にすることなく新たなノードを接続することが可能となっている。

【 0 0 5 7 】

一方、情報伝送の態様については、100Mbps (bit per second) 乃至400Mbpsの範囲で高速伝送が可能であり、更にリアルタイム伝送、双方向伝送及び多チャンネル伝送により多種の情報を双方向に伝送することが可能となっている。

【 0 0 5 8 】

また、各ノードの接続の形態については、図1 (a) に示す情報システムJのように、例えば、パーソナルコンピュータPCをルートノード（上述したように

、ツリー状トポロジにおける頂点のノード)として、CDプレーヤCP、MD (Mini Disc) プレーヤMP、デジタルビデオカメラDVC、プリンタPR、LD (LASER Disc) プレーヤLP、チューナT、スピーカSP、アンプAP、テレビジョン装置TV、ディジタルビデオテープレコーダVT、DVDプレーヤDV及び放送電波受信用のセットトップボックスSB等の種々の電気製品をシリアルバスBにより夫々接続し、これらをパーソナルコンピュータPCにより統括して制御することが可能となっている。

【0059】

ここで、当該シリアルバス規格においては、一つの系(シリアルバスBでツリー状に接続されている系)の中に含むことが可能な情報処理装置(上記ノードに相当する。)の数は最大で63個であり、更に、一つの系の中に二つのノード間の接続を最大で16個まで含ませることができる。なお、当該一つの系内で複数のノードNDを図1(b)に示すようにループ状に接続することは規格上禁止されている。

【0060】

次に、実際の伝送形態について、具体的に例示しつつ説明する。

【0061】

始めに、図2(a)に示すように、デジタルビデオカメラDVC、ディジタルビデオテープレコーダVT、パーソナルコンピュータPC及びセットトップボックスSBが夫々ノードとして相互にシリアルバスBにより接続され、情報伝送を行っているとする。より具体的には、デジタルビデオカメラDVCからはビデオデータを、ディジタルビデオテープレコーダVTからは所定の制御コマンドを、パーソナルコンピュータPCからは同様に他の機器を制御するための制御コマンドを、セットトップボックスSBからは受信した放送電波に含まれていた画像データ(例えば、MPEG(Moving Picture Expert Group)規格により圧縮されたMPEGデータを、夫々シリアルバスB上に送出しているとする。

【0062】

この場合、シリアルバスB上における送出された各情報の伝送形態としては、図2(b)に示すように、夫々のノードからの情報が、シリアルバスB上を時分

割的に夫々占有しつつ伝送される。そして、各情報は、 $125\mu\text{sec}$ の長さを有するシリアルバスB上の同期単位である上記アイソクロナスサイクルIC内に挿入されて伝送される。

【0063】

次に、上記アイソクロナスサイクルIC内のデータ構造について、図3を用いて説明する。

【0064】

先ず、図3に示すように、アイソクロナスサイクルICは、全てのノードの基準時刻を合わせるためにアイソクロナスサイクルICの先頭に常に挿入されるサイクルスタートパケットCSPと、複数チャンネル分のアイソクロナスパケットIPにより構成され、時間的に同期した情報が夫々のアイソクロナスパケットIPに含まれることにより構成されているアイソクロナス伝送領域ICTと、非同期の情報（例えば、種々の制御情報及び当該各制御情報に対応する応答情報等）が含まれているアシンクロナス伝送領域ACTと、により構成されている。

【0065】

また、各アイソクロナス伝送領域ICTの最後尾及びアシンクロナス伝送領域ACTの最後尾には、一のアイソクロナス伝送領域ICTの終了又は一のアシンクロナス伝送領域ACTの終了を示す時間的間隙であるサブアクションギャップSGが挿入されている。更に、各アイソクロナスパケットIPの間及びサイクルスタートパケットCSPと先頭のアイソクロナスパケットIPの間には、夫々のパケットの終了を示す時間的間隙であるアイソクロナスギャップIGが挿入されている。このとき、上記サブアクションギャップSGの長さはアイソクロナスギャップIGの長さよりも長く設定されている。

【0066】

次に、一のアイソクロナスパケットIPは、各アイソクロナスパケットIP内のデータ量を示す情報や各アイソクロナスパケットIP内の情報を伝送するチャンネルを示す情報等を含むIP (Isochronous Packet) ヘッダIPHと、CIPヘッダCIPHと、実際の映像情報又は音声情報を含むデータ領域DFと、により構成されている。

【 0 0 6 7 】

一方、アシンクロナス伝送領域 A C T は、各ノードからの情報の送出を行った旨の意志表示を当該各ノードが行うための時間的間隙であるアービトレーションリセットギャップ A P G と、非同期に伝送される制御情報等のデータが含まれるデータパケット D P と、送信先のノードからの返信に用いられるデータが含まれるアクノリッジパケット A C P とにより構成されている。ここで、データパケット D P とアクノリッジパケット A C P との間には、一のデータパケット D P の終了を示す時間的間隙であるアシンクロナスギャップ A G が挿入されている。

【 0 0 6 8 】

次に、一のデータパケット D P は、各データパケット D P の宛先を示す情報を含む A P (Asynchronous Packet) ヘッダ A P H と、アシンクロナス伝送領域 A C T を占有するデータパケット D P の伝送占有時間を示す情報及び占有するチャンネルを示す情報又は実際の制御情報等を含むデータ領域 A D F と、により構成されている。

【 0 0 6 9 】

上記したシリアルバス規格によれば、パーソナルコンピュータ等の情報処理装置から高速に制御情報を伝送することにより、家庭電化製品又は D V D プレーヤ等の音響映像装置等を一元的に制御することが可能となると共に、各ノード間でも画像情報又はオーディオ情報等を迅速且つ正確に相互伝送することが可能となる。

【 0 0 7 0 】

(II) 実施形態

次に、上述したシリアルバス規格により音楽情報等を含む記録情報が伝送される実施形態に係る情報伝送システムについて、図 4 を用いて説明する。

【 0 0 7 1 】

図 4 に示すように、実施形態の情報伝送システム S は、外部から放送電波を介して送信されてくる記録情報 S i n を受信し、後述する処理を施してレコーダ R に出力する情報送信装置としてのセットトップボックス B X と、当該セットトップボックス B X と I E E E 1 3 9 4 規格に準拠した伝送手段としてのシリアルバス

Bにより接続されていると共に、当該出力された記録情報SinをDVD-R1に記録する情報受信装置としての上記レコーダRと、により構成されている。

【0072】

また、セットトップボックスBXは、フロントエンド部20と、デスクランブラ21と、デマルチプレクサ22と、音声デコーダ23と、画像デコーダ24と、CPU25と、メモリ26と、抽出部27と、変換回路28と、第1暗号化手段としての暗号化部29と、第1授受手段、第2授受手段、第1送信手段及び第2送信手段としてのインタフェース部30と、により構成されており、当該各構成部材はバス31を介して相互に制御情報等の授受が可能とされている。

【0073】

更に、インタフェース部30は、コントローラ30Aと、第2暗号化手段としてのDTCP暗号化部30Bと、リンク層形成部30Cと、物理層形成部30Dと、付随するメモリ32と、により構成されている。

【0074】

一方、レコーダRは、ピックアップ2と、アンプ3と、復調部4と、復号化部5と、音声デコーダ6と、画像デコーダ7と、メモリ8と、記録手段としてのCPU9と、変調部10と、暗号化部11と、音声エンコーダ12と、画像エンコーダ13と、第1授受手段、第2授受手段、第1取得手段及び第2取得手段としてのインタフェース部14と、メモリ16と、第1解読手段としての解読部17と、により構成されており、メモリ16及び解読部17を除く各構成部材はバス15を介して相互に制御情報等の授受が可能とされている。

【0075】

また、インタフェース部14は、コントローラ14Aと、第2解読手段としてのDTCP復号部14Bと、リンク層検出部14Cと、物理層検出部14Dと、により構成されている。

【0076】

次に、セットトップボックスBX及びレコーダRにおける動作について説明する。

【0077】

(i) 一般動作

始めに、本発明に係る部分以外の一般的な動作について説明する。

【 0 0 7 8 】

なお、実施形態のセットトップボックス B X は、上述した如くレコーダ R への記録情報の伝送に加えて、受信した音楽情報等の図示しないテレビジョン装置等への出力も可能とされている。

【 0 0 7 9 】

また、実施形態のレコーダ R は、セットトップボックス B X から伝送された記録情報を DVD-R 1 に記録するだけでなく、セットトップボックス B X 以外の他の装置から出力された記録情報 S_{inn} を DVD-R 1 に記録すると共に、当該 DVD-R 1 にそれまでに記録されている音楽情報等を再生し、出力信号 S_{out} として外部に出力することも可能とされている。

【 0 0 8 0 】

先ず、セットトップボックス B X において、外部から入力される記録情報 S_{in} を上記図示しないテレビジョン装置に出力する場合の動作について説明する。

【 0 0 8 1 】

この場合に、当該記録情報 S_{in} には、上記音楽情報と共に画像情報が含まれており、これらの各情報は夫々圧縮されると共に暗号化されて入力される。

【 0 0 8 2 】

そして、フロントエンド部 2 0 は、当該記録情報 S_{in} に対して予め設定された受信処理を施し、受信信号 S_{fe} を生成してデスクランブラ 2 1 に出力する。

【 0 0 8 3 】

次に、デスクランブラ 2 1 は、当該受信信号 S_{fe} に含まれている音声情報及び画像情報における暗号化を解読し、解読信号 S_{ds} を生成してデマルチプレクサ 2 2 へ出力する。

【 0 0 8 4 】

これにより、デマルチプレクサ 2 2 は、解読信号 S_{ds} 内に含まれている音声情報と画像情報とを分離し、当該分離した音声情報を音声信号 S_{as} として音声デコーダ 2 3 へ出力すると共に、更に当該分離した画像情報を画像信号 S_{vs} として画

像デコーダ 2 4 へ出力する。

【 0 0 8 5 】

そして、音声デコーダ 2 3 は、当該音声信号 S a s を復号し、音声出力信号 S a d として図示しないテレビジョン装置へ出力する。

【 0 0 8 6 】

他方、画像デコーダ 2 4 は、当該画像信号 S v s を復号し、画像出力信号 S v d として同じく図示しないテレビジョン装置へ出力する。

【 0 0 8 7 】

このとき、CPU 2 5 は、バス 3 1 を介して必要な制御情報の授受を行いつつ上記各構成部材を統括制御する。また、当該統括制御に必要な情報はバス 3 1 を介して一時的にメモリ 2 6 に記憶されつつ当該統括制御に用いられる。

【 0 0 8 8 】

次に、レコーダ R において、外部から入力される記録情報 S i n n を DVD - R 1 に記録する場合の動作について説明する。

【 0 0 8 9 】

この場合にも、当該記録情報 S i n n には、音楽情報と共に画像情報が含まれて入力される。

【 0 0 9 0 】

そして、画像エンコーダ 1 3 は、当該記録情報 S i n n における画像情報に対して予め設定された変調処理及び暗号化処理を施し、記録用の画像情報を生成する。

【 0 0 9 1 】

また、音声エンコーダ 1 2 は、当該記録情報 S i n n における音声情報に対して上記画像情報に対する変調処理に対応する変調処理及び暗号化処理を施し、記録用の音声情報を生成する。

【 0 0 9 2 】

次に、暗号化部 1 1 は、上記記録用の画像情報及び記録用の音声情報を含む記録信号 S e v に対して予め設定された DVD - R 1 への記録用の暗号化処理（具体的には、いわゆる S D M I (Secure Digital Music Initiative) 規格に基づ

く暗号化処理等)を施し、暗号化記録信号 S_{ar} を生成して変調部 10 へ出力する。

【0093】

そして、変調部 10 は、当該暗号化記録信号 S_{ar} に基づいて、ピックアップ 2 内に設けられた記録用の光ビーム B を DVD-R 1 に対して照射するための図示しない半導体レーザを駆動して、当該暗号化記録信号 S_{ar} に含まれている記録すべき情報に対応して強度変化する当該光ビーム B を射出させるための強度制御信号 S_d を生成してピックアップ 2 に出力する。

【0094】

その後、ピックアップ 2 は、当該強度制御信号 S_d に基づいて上記図示しない半導体レーザを駆動し、記録用の光ビーム B を射出して DVD-R 1 に対する上記画像情報及び音声情報の記録を行う。

【0095】

このとき、CPU 9 は、バス 15 を介して必要な制御情報の授受を行いつつ上記各構成部材を統括制御する。また、当該統括制御に必要な情報はバス 15 を介して一時的にメモリ 8 に記憶されつつ当該統括制御に用いられる。

【0096】

以上の一連の動作により、記録情報 S_{inn} に含まれている各情報が DVD-R 1 上に記録されることとなる。

【0097】

次に、レコーダ R において、DVD-R 1 に既に記録されている記録情報を再生する場合の動作について説明する。

【0098】

当該再生時においては、ピックアップ 2 は、再生用の一定強度の光ビーム B を射出し、その反射光を図示しない受光部で受光して、当該反射光の強度変化に対応して変化する検出信号を生成してアンプ 3 へ出力する。

【0099】

次に、アンプ 3 は、当該検出信号に対して予め設定された増幅処理及び波形整形処理等を施し、再生信号 S_p を生成して復調部 4 へ出力する。

【0100】

そして、復調部4は、再生信号Spに対して予め設定された復調処理を施し、復調信号Sdmを生成して復号化部5へ出力する。

【0101】

次に、復号化部5は、当該復調信号Sdmに含まれている音声情報及び画像情報における暗号化を解読し、解読信号Sdcを生成して音声デコーダ6及び画像デコーダ7へ出力する。

【0102】

これにより、音声デコーダ6は、解読信号Sdcに含まれている音声情報を復号し、復号音声情報を生成する。

【0103】

また、画像デコーダ7は、解読信号Sdcに含まれている画像情報を復号し、復号画像情報を生成する。

【0104】

そして、当該復号された復号音声情報及び復号画像情報は、復号出力信号Sou tとして図示しないテレビジョン装置等に纏めて出力される。

【0105】

このとき、CPU9は、バス15を介して必要な制御情報の授受を行いつつ上記各構成部材を統括制御する。また、当該統括制御に必要な情報はバス15を介して一時的にメモリ8に記憶されつつ当該統括制御に用いられる。

【0106】

以上の一連の動作により、DVD-R1に記録されている記録情報が再生されて外部に出力されることとなる。

【0107】

(ii) 本発明に係る動作

次に、本発明に係るセットトップボックスBX及びレコーダRの動作について説明する。

【0108】

セットトップボックスBXにおいて受信した記録情報SinをレコーダRに伝送

し、更にDVD-R1に記録する場合には、始めに、セットトップボックスBXに対して記録情報Sinが入力されると、上記したフロントエンド部20及びデスクランブラ21の動作により、上記解読信号Sdsが生成され、抽出部27に出力される。

【0109】

これにより、抽出部27は、当該解読信号SdsからDVD-R1に記録すべき記録情報のみを抽出し、抽出信号Sdvとして変換回路28へ出力する。

【0110】

そして、変換回路28は、当該抽出信号Sdvにおけるフォーマット形式をDVD-R1へ記録するための記録フォーマット形式に変換し、変換信号Smvを生成して暗号化部29へ出力する。

【0111】

次に、暗号化部29は、CPU25に格納されている予め設定されている暗号化用の暗号処理情報ECを読み出し、これに含まれている予め設定された暗号化キー並びに暗号化テーブルを用いて予め設定されている暗号化処理により変換信号Smvを暗号化し、暗号化信号Sxを生成してインタフェース部30へ出力する。

【0112】

なお、図4においては、当該暗号処理情報ECの流れを破線で示している。

【0113】

これと並行して、当該暗号化部29は、変換信号Smvの暗号化に用いた上記暗号処理情報ECをそのままインタフェース部30へ出力する。

【0114】

そして、インタフェース部30内のコントローラ30Aは、メモリ32との間で必要な情報の授受をメモリ信号Smとして実行しつつ、暗号化信号Sxをそのままリンク層形成部30Cに出力すると共に、暗号処理情報ECをそのままDTCP暗号化部30Bへ出力する。

【0115】

これにより、DTCP暗号化部30Bは、上記DTCP規格に準拠した暗号化

方法により暗号処理情報 E C 自体を暗号化し、暗号化処理情報 S a e を生成してリンク層形成部 3 0 C へ出力する。

【 0 1 1 6 】

そして、リンク層形成部 3 0 C は、シリアルバス規格に準拠して暗号化信号 S x 及び暗号化処理情報 S a e に含まれるデータを用いてアイソクロナスサイクル I C としてのリンク層を形成し、リンク信号 S l k を生成して物理層形成部 2 4 へ出力する。

【 0 1 1 7 】

このとき、当該形成されるアイソクロナスサイクル I C においては、暗号化信号 S x がアシンクロナス伝送領域 A C T 内のデータパケット D P 内に格納されて伝送されるように当該リンク層が形成されると共に、暗号化処理情報 S a e がアイソクロナス伝送領域 I C T 内のいずれかのアイソクロナスパケット I P 内に格納されて伝送されるように当該リンク層が形成される。

【 0 1 1 8 】

これらにより、物理層形成部 2 4 は、シリアルバス規格に準拠してリンク信号 S l k に含まれるデータを用いてアイソクロナスサイクル I C としての物理層を形成し、最終的に当該アイソクロナスサイクル I C を生成してシリアルバス B を介してレコーダ R に出力する。

【 0 1 1 9 】

このとき、データパケット D P 内に格納されて伝送される暗号化信号 S x は、シリアルバス規格における最大伝送速度（例えば、4 0 0 Mbps）を用いて伝送されるが、アイソクロナスパケット I P 内に格納されて伝送される暗号化処理情報 S a e は、当該アイソクロナスパケット I P による伝送が上記 D T C P 規格に準拠しなければならないこととされている関係上、DVD-R 1 への記録後の再生時における再生速度と同様の伝送速度により伝送される。

【 0 1 2 0 】

これらの動作と並行して、C P U 2 5 は、バス 3 1 を介して必要な制御情報の授受を行いつつインタフェース部 3 0 を含む上記各構成部材の制御を行う。

【 0 1 2 1 】

次に、当該アイソクロナスサイクル I C をシリアルバス B から受信したレコーダ R においては、先ず、インタフェース部 1 4 内の物理層検出部 1 4 D が、当該受信したアイソクロナスサイクル I C 内の各物理層を検出し、リンク層としての当該アイソクロナスサイクル I C を復元し、リンク信号 S lk を生成してリンク層検出部 1 4 C へ出力する。

【 0 1 2 2 】

そして、リンク層検出部 1 4 C は、当該リンク信号 S lk から上記アイソクロナスパケット I P 及びデータパケット D P を分離抽出し、当該データパケット D P 内に格納されている上記暗号化信号 S x をコントローラ 1 4 A に出力すると共に、上記アイソクロナスパケット I P に格納されている暗号化処理情報 S ae を D T C P 復号部 1 4 B へ出力する。

【 0 1 2 3 】

これにより、D T C P 復号部 1 4 B は、暗号化処理情報 S ae に対して上記 D T C P 暗号化部 3 0 B における暗号化処理に対応した D T C P 規格に準拠した解読処理を施し、上記暗号化処理情報 E C を復元してコントローラ 1 4 A へ出力する。

【 0 1 2 4 】

そして、コントローラ 1 4 A は、メモリ 1 6 との間で必要な情報の授受をメモリ信号 S m として実行しつつ、暗号化信号 S x 及び暗号化処理情報 E C を共にそのまま解読部 1 7 に出力する。

【 0 1 2 5 】

次に、解読部 1 7 は、当該暗号化処理情報 E C を用いて、上記暗号化部 2 9 における暗号化処理に対応する解読処理を暗号化信号 S x に対して施し、元の上記変換信号 S mv を復元して暗号化部 1 1 へ出力する。

【 0 1 2 6 】

これ以後は、上記暗号化部 1 1 及び変調部 1 0 において、変換信号 S mv に含まれる記録情報に対する暗号化処理（D V D - R 1 に記録されていた当該 D V D - R 1 を個別識別するための識別情報に基づく暗号化処理）及び変調処理（上記した一般動作の場合と同様の強度制御信号 S d の生成処理）が施され、その後、ピックアップ 2 によりセットトップボックス B X から伝送されてきた当該記録情報

がDVD-R1に記録されることとなる。

【0127】

このとき、CPU9は、バス15を介して必要な制御情報の授受を行いつつ上記記録動作を統括制御する。

【0128】

以上の一連の動作により、セットトップボックスBXにおいて受信された記録情報Sinに含まれている各情報がDVD-R1上に記録される。

【0129】

以上説明したように、実施形態に係るセットトップボックスBX及びレコーダRの動作によれば、レコーダRに伝送すべき記録情報を暗号化した暗号化信号SxをデータパケットDPを用いて高速に伝送すると共に、当該暗号化に用いられた暗号処理情報EC（暗号化キー及び暗号化テーブル）を暗号化した暗号化処理情報SaeをアイソクロナスパケットIPを用いて伝送するので、当該記録情報を暗号化された状態で高速且つ大量に送信することができる。

【0130】

また、伝送前に記録情報が暗号化されているので、当該記録情報の秘匿性を高めつつレコーダRに伝送することができる。

【0131】

(III) 変形形態

次に、本発明に係る変形形態について説明する。

【0132】

上述した実施形態においては、暗号処理情報ECが予めセットトップボックスBXのCPU25内に備えられている場合について説明したが、これ以外に、以下のような態様で情報を授受する場合に本発明を適用することもできる。

【0133】

すなわち、先ず、上記DVD-R1個々を他のDVD-Rから識別するための上記識別情報をレコーダRにおいて当該DVD-R1から検出し、これを（必要に応じて当該レコーダRにおいて暗号化した上で）アイソクロナスパケットIPを用いてセットトップボックスBXに伝送する。

【 0 1 3 4 】

次に、セットトップボックス B X においては当該識別情報を（それが暗号化されている場合はこれを解読した上で）暗号処理情報 E C（暗号化キー）として用いて上記変換信号 S_{mv}を暗号化して上記暗号化信号 S_xを生成し、これをデータパケット D P を用いてレコーダ R に高速に伝送（返信）した後に当該レコーダ R において D V D - R 1 に記録するのである。

【 0 1 3 5 】

このような変形形態による場合でも、レコーダ R に伝送すべき記録情報の暗号化に用いられる識別情報をアイソクロナスパケット I P を用いてセットトップボックス B X に伝送すると共に、これを用いて暗号化された暗号化信号 S_xをデータパケット D P を用いて高速にレコーダ R に返信するので、当該記録情報を暗号化された状態で高速且つ大量に送信することができることとなる。

【 0 1 3 6 】

このとき、上述した変形形態において、セットトップボックス B X における識別情報を用いた暗号化の際に、当該暗号化方法を D V D - R 1 に情報を記録する際に暗号化部 1 1 において用いられる暗号化処理方法と同様の方法とすれば、レコーダ R においては返信されてきた暗号化信号 S_xをそのまま直接 D V D - R 1 に記録すれば足りることとなるので、より簡便且つ高速に記録情報をレコーダ R に伝送して D V D - R 1 に記録することができる。

【 0 1 3 7 】

なお、上述の実施形態及び変形形態においては、レコーダ R において D V D - R 1 に記録情報を記録する場合について説明したが、これ以外に、D V D - R W（DVD - Re - Recordable）又は D V D - R A M（DVD - Random Access Memory）等の他の光ディスク、或いは半導体メモリ等の固体メモリをレコーダ R における記録媒体として用いることもできる。

【 0 1 3 8 】

また、上述した一連の記録処理を各 C P U 9 及び 2 5 において統括制御するための制御プログラムを情報記録媒体としてのフレキシブルディスク又はハードディスク等の記録しておき、コンピュータとしてのマイクロプロセッサ等によりこ

れを読み出して実行することにより、一般のパーソナルコンピュータ又はサーバ等を上記CPU9又は25として機能させることも可能である。

【0139】

更に、上述したセットトップボックスBXをシリアルバスBを介して記録情報を再生する機能のみを有するプレーヤに伝送し、当該プレーヤにおいて伝送された記録情報を再生・出力するように構成することもできる。

【0140】

【発明の効果】

以上説明したように、請求項1に記載の発明によれば、暗号化特定情報を高速の第1伝送態様で送受信すると共に、暗号処理情報を第2伝送態様で送受信するので、情報処理装置間で送受信すべき特定情報を暗号化された状態で高速且つ大量に送受信することができる。

【0141】

また、送信前に特定情報が暗号化されるので、当該特定情報の秘匿性を高めつつ送信することができる。

【0142】

請求項2に記載の発明によれば、暗号化特定情報を高速の第1伝送態様で送受信すると共に、暗号処理情報を第2伝送態様で送受信するので、情報処理装置間で送受信すべき特定情報を暗号化された状態で高速且つ大量に送受信することができる。

【0143】

また、送信前に特定情報が暗号化されるので、当該特定情報の秘匿性を高めつつ送信することができる。

【0144】

請求項3に記載の発明によれば、送信すべき特定情報を暗号化した暗号化特定情報を高速の第1伝送態様で送信すると共に、当該暗号化に用いられた暗号処理情報を暗号化した暗号化処理情報を第2伝送態様で送信するので、当該特定情報を暗号化された状態で高速且つ大量に送信することができる。

【0145】

また、送信前に特定情報が暗号化されているので、当該特定情報の秘匿性を高めつつ情報受信装置に送信することができる。

【 0 1 4 6 】

請求項 4 に記載の発明によれば、請求項 3 に記載の発明の効果に加えて、特定情報が A V 情報であると共に、暗号処理情報が当該 A V 情報を暗号化するための暗号化キー及び暗号化テーブルであるので、必要な A V 情報を秘匿性を高めつつ高速且つ大量に送信することができる。

【 0 1 4 7 】

請求項 5 に記載の発明によれば、請求項 3 又は 4 に記載の発明の効果に加えて、 I E E E 1 3 9 4 規格に準拠したアイソクロナス伝送モードで暗号化特定情報を送信するので、当該特定情報を I E E E 1 3 9 4 規格における最大伝送速度で情報受信装置に送信することができる。

【 0 1 4 8 】

請求項 6 に記載の発明によれば、送信すべき特定情報を暗号化した暗号化特定情報を高速の第 1 伝送態様で送信すると共に、当該暗号化に用いられた暗号処理情報を暗号化した暗号化処理情報を第 2 伝送態様で送信するので、当該特定情報を暗号化された状態で高速且つ大量に送信することができる。

【 0 1 4 9 】

また、送信前に特定情報が暗号化されているので、当該特定情報の秘匿性を高めつつ情報受信装置に送信することができる。

【 0 1 5 0 】

請求項 7 に記載の発明によれば、取得された暗号化処理情報を解読して得られた暗号処理情報を用いて取得された暗号化特定情報を解読するので、高速且つ大量に特定情報を受信することができると共に、特定情報の秘匿性を高めつつこれを受信することができる。

【 0 1 5 1 】

請求項 8 に記載の発明によれば、請求項 7 に記載の発明の効果に加えて、生成された特定情報を記録媒体に記録するので、秘匿性の高い特定情報を高速に取得して記録媒体に記録することができる。

【 0 1 5 2 】

請求項 9 に記載の発明によれば、取得された暗号化処理情報を解読して得られた暗号処理情報を用いて取得された暗号化特定情報を解読するので、高速且つ大量に特定情報を受信することができると共に、特定情報の秘匿性を高めつつこれを受信することができる。

【 0 1 5 3 】

請求項 1 0 に記載の発明によれば、特定情報を暗号化した暗号化特定情報を高速の第 1 伝送態様で送受信すると共に、当該暗号化に用いられた暗号処理情報を暗号化した暗号化処理情報を第 2 伝送態様で送受信するので、当該特定情報を暗号化された状態で高速且つ大量に送受信することができる。

【 0 1 5 4 】

また、送信前に特定情報が暗号化されると共に受診後にこれを解読して暗号化特定情報の解読に用いるので、当該特定情報の秘匿性を高めつつその送受信を実行することができる。

【 0 1 5 5 】

請求項 1 1 に記載の発明によれば、送信すべき特定情報を暗号化した暗号化特定情報を高速の第 1 伝送態様で送信すると共に、当該暗号化に用いられた暗号処理情報を暗号化した暗号化処理情報を第 2 伝送態様で送信するように送信コンピュータを機能させるので、当該特定情報を暗号化された状態で高速且つ大量に送信することができる。

【 0 1 5 6 】

また、送信前に特定情報が暗号化されるように送信コンピュータを機能させるので、当該特定情報の秘匿性を高めつつ情報受信装置に送信することができる。

【 0 1 5 7 】

請求項 1 2 に記載の発明によれば、取得された暗号化処理情報を解読して得られた暗号処理情報を用いて取得された暗号化特定情報を解読するように受信コンピュータを機能させるので、高速且つ大量に特定情報を受信することができると共に、特定情報の秘匿性を高めつつこれを受信することができる。

【図面の簡単な説明】

【図 1】

IEEE 1394 規格により接続された電気製品（ノード）の例を示す図であり、（a）はシリアル接続された電気機器の例を示す図であり、（b）はループ接続を示す図である。

【図 2】

シリアルバス上の伝送形態を例示する図である。

【図 3】

アイソクロナスサイクルの構成を示す図である。

【図 4】

実施形態の情報伝送システムの概要構成を示すブロック図である。

【符号の説明】

- 1 … DVD-R
- 2 … ピックアップ
- 3 … アンプ
- 4 … 復調部
- 5 … 復号化部
- 6 … 音声デコーダ
- 7 … 画像デコーダ
- 8、16、26、32 … メモリ
- 9、25 … CPU
- 10 … 変調部
- 11 … 暗号化部
- 12 … 音声エンコーダ
- 13 … 画像エンコーダ
- 14、30 … インタフェース部
- 14A、30A … コントローラ
- 14B … DTCF 復号部
- 14C … リンク層検出部
- 14D … 物理層検出部

1 5、3 1…バス
1 7…解読部
2 0…フロントエンド部
2 1…デスクランブラ
2 2…デマルチプレクサ
2 3…音声デコーダ
2 4…画像デコーダ
2 7…抽出部
2 8…変換回路
2 9…暗号化部
3 0 B…D T C P 暗号化部
3 0 C…リンク層形成部
3 0 D…物理層形成部
S…情報伝送システム
J…情報システム
B X、S B…セットトップボックス
E C…暗号処理情報
B…シリアルバス
R…レコーダ
N D…ノード
P C…パーソナルコンピュータ
C P…C D プレーヤ
M P…M D プレーヤ
D V C…デジタルビデオカメラ
P R…プリンタ
L P…L D プレーヤ
T…チューナ
S P…スピーカ
A P…アンプ

TV…テレビジョン装置
VT…デジタルビデオテープレコーダ
DV…DVDプレーヤ
IC…アイソクロナスサイクル
CSP…サイクルスタートパケット
ICT…アイソクロナス伝送領域
ACT…アシンクロナス伝送領域
APG…アービトレーションリセットギャップ
DP…データパケット
ACP…アクノリッジパケット
APH…APヘッダ
SG…サブアクションギャップ
IG…アイソクロナスギャップ
AG…アシンクロナスギャップ
IPH…IPヘッダ
IP…アイソクロナスパケット
CIPH…CIPヘッダ
Sin、Sinn…記録情報
Sout…出力信号
Sfe…受信信号
Sds、Sdc…解読信号
Sas…音声信号
Svs…画像信号
Sad…音声出力信号
Svd…画像出力信号
Sev…記録信号
Sar…暗号化記録信号
Sd…強度制御信号
Sp…再生信号

S_{dm}…復調信号

S_{out}…復号出力信号

S_{dv}…抽出信号

S_{mv}…変換信号

S_x…暗号化信号

S_{lk}…リンク信号

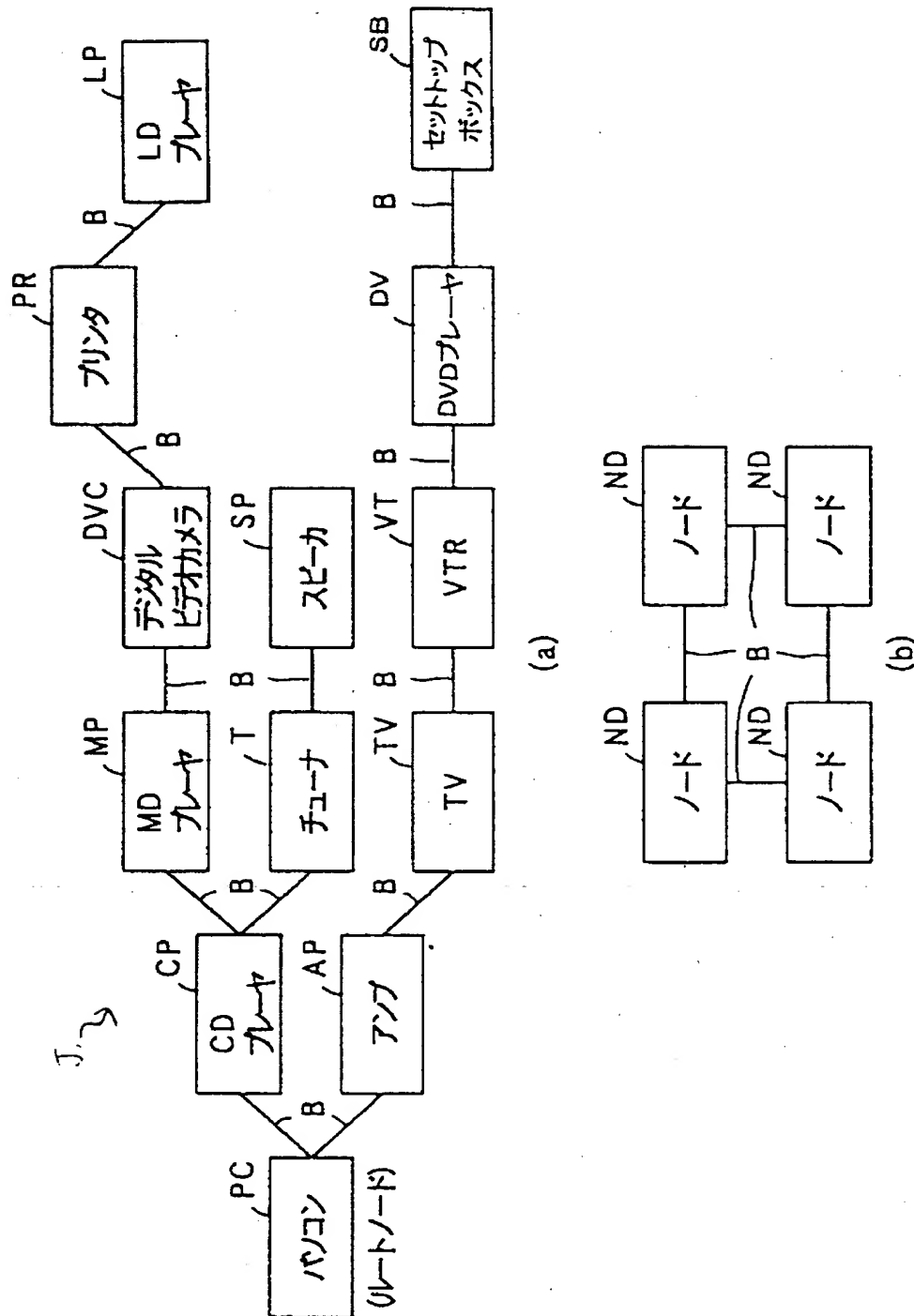
S_{ae}…暗号化処理情報

S_m…メモリ信号

【書類名】 図面

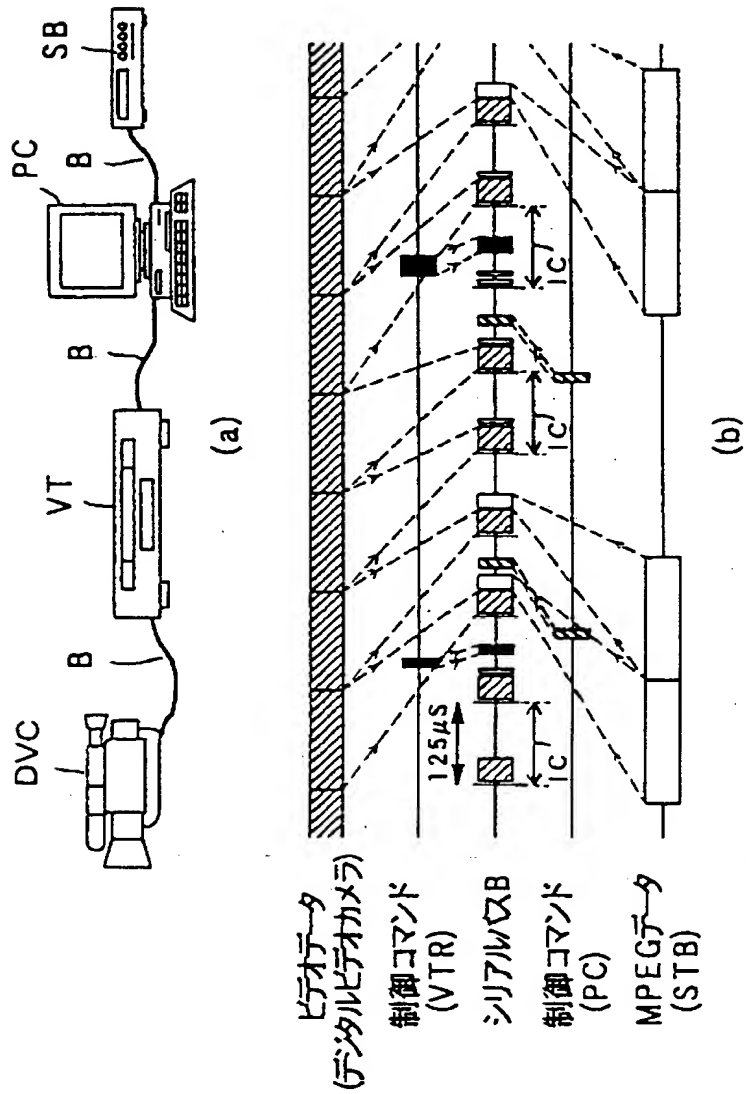
【図1】

IEEE1394規格により接続された電気製品（ノード）の例



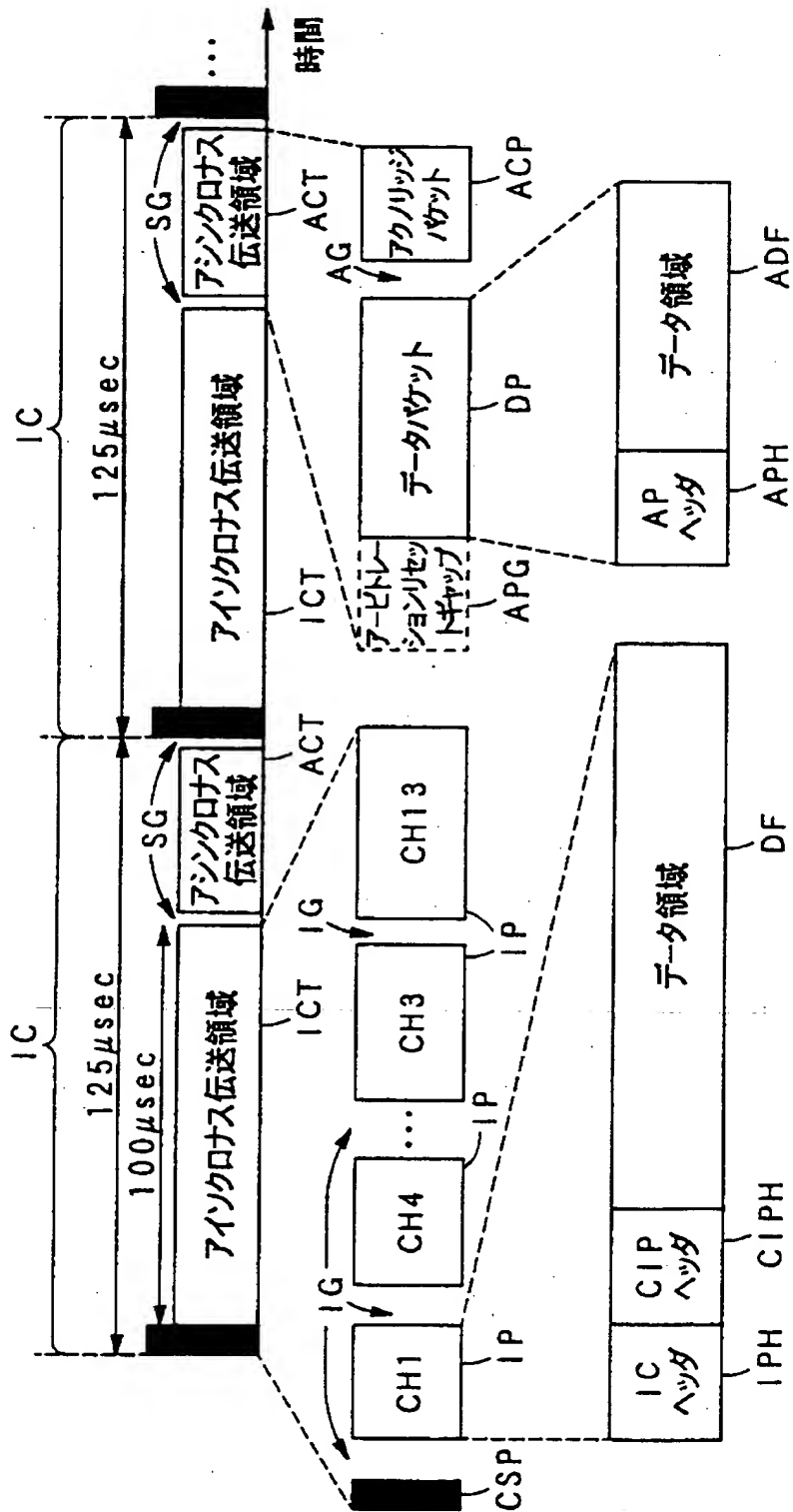
【図 2】

シリアルバス上の伝送形態



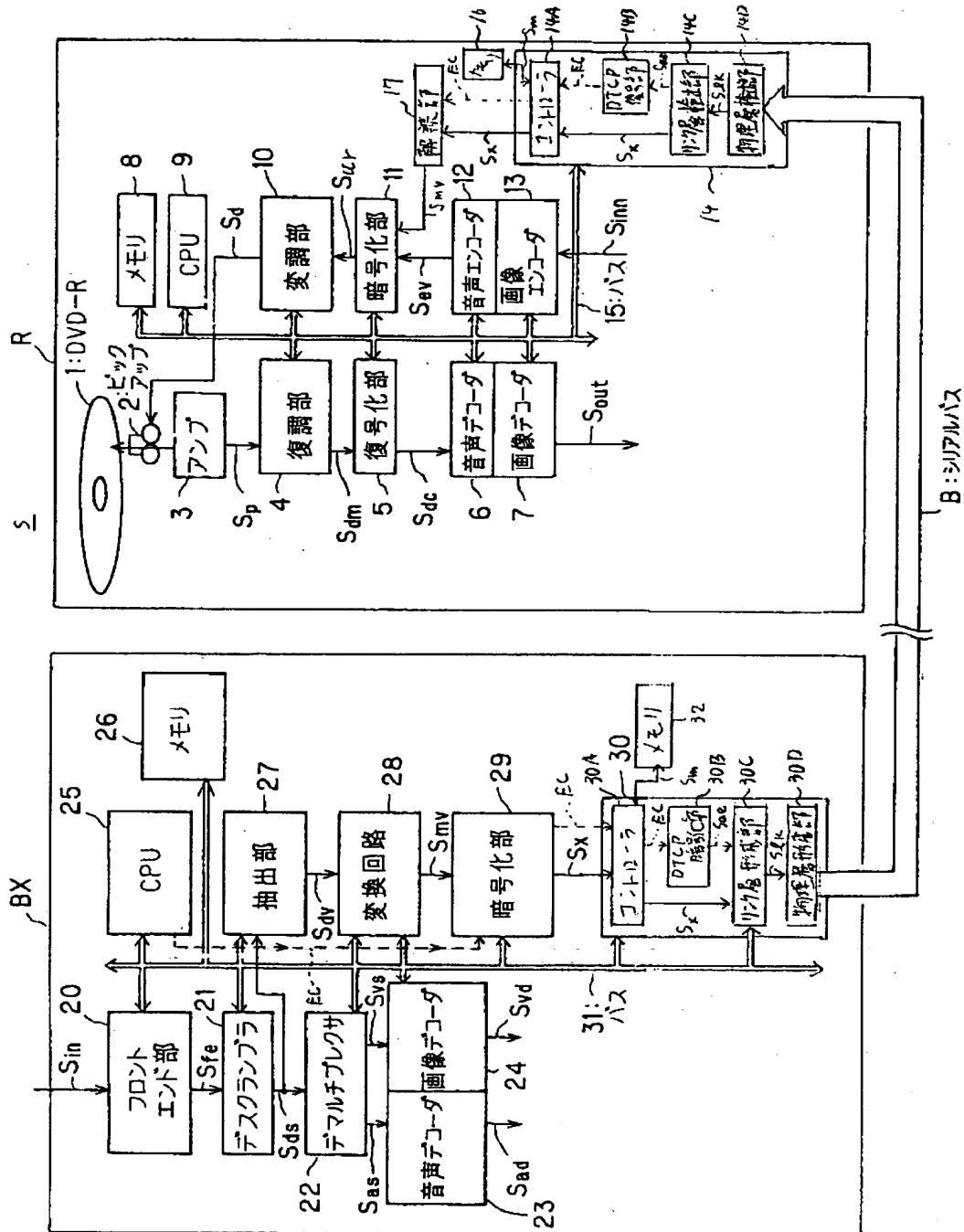
【図 3】

アイソクロナスサイクルの構成



【図 4】

実施形態の情報伝送システムの概要構成を示すブロック図



【書類名】 要約書

【要約】

【課題】 暗号処理情報を用いて暗号化された音楽情報等を伝送する場合に、当該音楽情報等を暗号化された状態で秘匿性を高めつつ高速且つ大量に伝送することが可能な情報送信装置及び情報受信装置等を提供する。

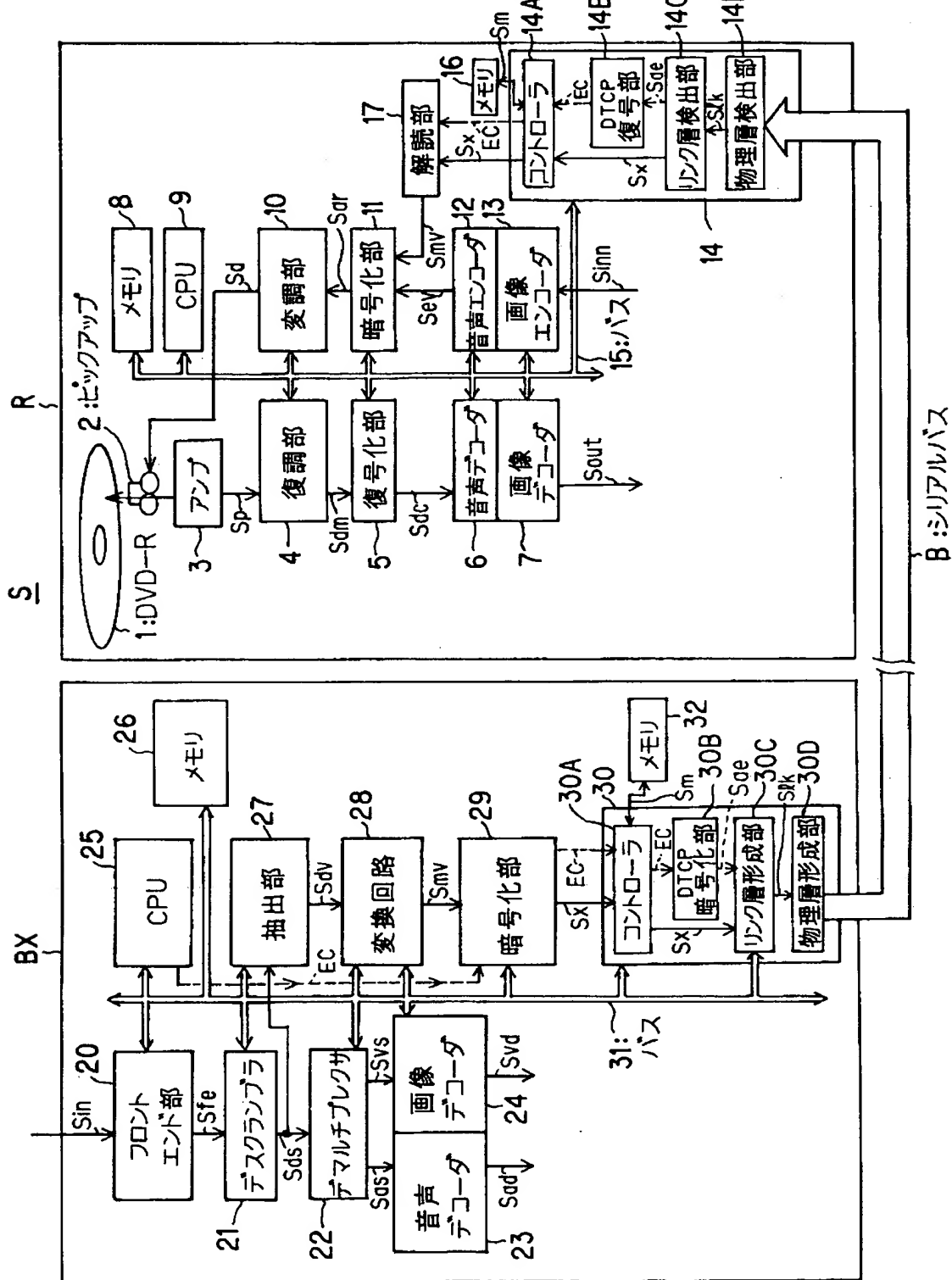
【解決手段】 暗号化された音楽情報等及びその暗号化に用いられた暗号処理情報自体を暗号化したものをセットトップボックスB XからレコーダRにシリアルバスBを介して伝送して当該音楽情報等をDVD-R 1に記録するに当たり、当該シリアルバスBが準拠する規格であるIEEE 1394規格におけるアシンクロナス伝送領域を用いて暗号化された音楽情報を高速に伝送し、他方、IEEE 1394規格におけるアイソクロナス伝送領域を用いて暗号化された暗号処理情報を一倍速で伝送する。

【選択図】 図4

【書類名】 手続補正書
【提出日】 平成12年 9月 7日
【あて先】 特許庁長官殿
【事件の表示】
 【出願番号】 特願2000-267612
【補正をする者】
 【識別番号】 000005016
 【氏名又は名称】 パイオニア株式会社
【代理人】
 【識別番号】 100083839
 【弁理士】
 【氏名又は名称】 石川 泰男
 【電話番号】 03-5443-8461
【手続補正 1】
 【補正対象書類名】 図面
 【補正対象項目名】 図 4
 【補正方法】 変更
 【補正の内容】 1
【プルーフの要否】 要

【図 4】

実施形態の情報伝送システムの概要構成を示すブロック図



出 願 人 履 歴 情 報

識別番号 [000005016]

1. 変更年月日 1990年 8月31日
[変更理由] 新規登録
住 所 東京都目黒区目黒1丁目4番1号
氏 名 パイオニア株式会社